(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 December 2004 (29.12.2004)

PCT

(10) International Publication Number
WO 2004/114698 A1

(51) International Patent Classification[7]: H04Q 7/24

(21) International Application Number:
PCT/KR2004/001497

(22) International Filing Date: 22 June 2004 (22.06.2004)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2003-0041145 24 June 2003 (24.06.2003) KR

(71) Applicant *(for all designated States except US)*: LG TELECOM, LTD. [KR/KR]; 679, Yoksam-dong, Kangnam-gu, Seoul 135-916 (KR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: JEON, Gwang-Sik [KR/KR]; 111-305, Seonsa Hyundai Apt., Amsa 2-dong, Gangdong-gu, Seoul 134-703 (KR).

(74) Agent: WONJON PATENT FIRM; 8th Floor, Poonglim Bldg., 823-1, Yeoksam-dong, Kangnam-gu, Seoul 135-784 (KR).

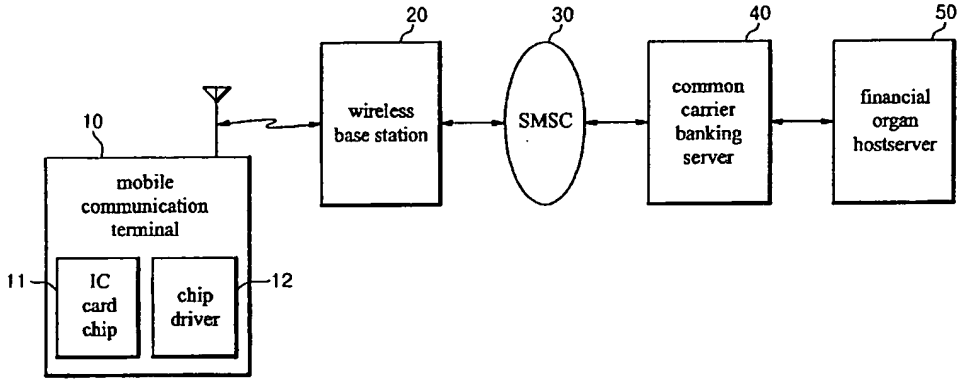
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR LOCKING/UNLOCKING MOBILE BANKING FUNCTION



(57) Abstract: A system and method for locking/unlocking a mobile banking function using a short message service (SMS) message is provided. Personal financial information stored in an IC card chip (for example, an embedded or external smart card chip or a traffic card chip) of a mobile communication terminal for storing personal financial information for supporting a banking function is maintained in a locking state using a short message service (SMS) message to disable access to the IC card chip or is unlocked to enable access to the IC card chip. Accordingly, when the mobile communication terminal is lost or stolen, an attempt for an illegal banking function using the IC card chip of the mobile communication terminal can be completely prevented, and a mobile communication terminal user does not need to visit a financial organ personally and needs to simply file a report to a corresponding financial organ or common carrier such that the use of an IC card chip of the mobile communication terminal can be stopped or the IC card chip can be reused.

WO 2004/114698 A1

SYSTEM AND METHOD FOR LOCKING/UNLOCKING MOBILE BANKING FUNCTION

Technical Field

The present invention relates to a system and method for locking/unlocking a mobile banking function, and more particularly, to a system and method for locking/unlocking a mobile banking function using a short message service (SMS) message.

Background Art

In general, a variety of mobile communication terminals such as mobile phones, PCS terminals, and PDA phones, support a variety of banking functions, such as user's card price inquiry and settlement, account balance inquiry, deposit transfer and remittance, and loan inquiry and redemption using an IC card chip, such as an embedded or external smart card chip or a traffic card chip in which personal financial information, such as a mobile communication terminal user (hereinafter, referred to as a user)'s account number for banking and a personal identification number (PIN) for user certification is stored.

Meanwhile, when a conventional mobile communication terminal for supporting a variety of banking functions as above is lost and stolen, if the user files a loss report or a theft report to a corresponding financial organ, in prior arts, personal financial information stored in a user's mobile communication IC card chip should be registered in a blacklist.

In actuality, when user certification for a specific mobile communication IC card chip is intended, a financial host determines whether or not the personal financial information stored in the mobile communication IC card chip for which user certification is intended is coincident with the personal financial information registered in the blacklist

of the financial host. In this case, if it is determined that the personal financial information stored in the mobile communication IC card chip for which user certification is intended is registered in the blacklist, the financial host restricts the personal financial information so that a banking function using the corresponding mobile communication IC card chip cannot be performed.

However, when the personal financial information stored in a specific user's mobile communication terminal IC card chip is registered in the blacklist of the financial host managed by the financial organ and the use thereof is restricted, there are inconveniences that the user should visit a corresponding financial organ personally, so as to request the reuse or unlocking of the personal financial information stored in own mobile communication terminal IC card chip registered in the blacklist. As such, the IC card chip cannot be reused.

Disclosure

To solve the above-described problems, the present invention provides a system and method for locking/unlocking a mobile banking function in which when there is a user's request caused by a mobile communication terminal loss or theft accident, personal financial information stored in an IC card chip of a mobile communication terminal for storing personal financial information for supporting a banking function is maintained in a locking state using a short message service (SMS) message to disable access to the IC card chip or is unlocked to enable access to the IC card chip.

According to an aspect of the present invention, there is provided a system for locking/unlocking a mobile banking function, the system comprising a mobile communication terminal, which includes an embedded or external IC card chip in which

personal financial information for supporting a banking function is stored, when the mobile communication terminal receives a chip blocking SMS message for maintaining the personal financial information stored in the IC card chip in a locking state, the mobile communication terminal restricting access to the IC card chip by driving an internal chip driver, and when the mobile communication terminal receives a chip blocking unlocking SMS message for unlocking the locking state of the personal financial information, the mobile communication terminal permitting access to the IC card chip by driving the chip driver; a common carrier banking server, which communicates with the mobile communication terminal via a wireless base station and a short message service center (SMSC) and transmits a chip blocking SMS message or a chip blocking unlocking SMS message to the mobile communication terminal when receiving a chip blocking or chip blocking unlocking request from a financial organ issuing the IC card chip; and a financial organ host, which transmits a chip blocking request to the common carrier banking server when receiving a theft and loss report from a user of the mobile communication terminal, and which transmits a chip blocking unlocking request to the common carrier banking server when receiving a request for the reuse of the mobile communication terminal for which a theft and loss report has been filed from the user.

According to another aspect of the present invention, there is provided a method of locking/unlocking a mobile banking function, the method comprising when receiving a theft and loss report of a mobile communication terminal from a user of the mobile communication terminal or receiving a request for the reuse of the mobile communication terminal for which the theft and loss report has been filed from the user, requesting chip blocking or chip blocking unlocking of a common carrier banking server; transmitting a chip blocking short message service message or a chip blocking unlocking SMS message

to the corresponding mobile communication terminal via a wireless base station and a PSDN; determining whether or not the SMS message received from the common carrier banking server is the chip blocking SMS message or the chip blocking unlocking SMS message; if it is determined that the SMS message received by the mobile communication terminal is the chip blocking SMS message, driving an internal chip driver of the mobile communication terminal to restrict access to an embedded or external IC card chip of the mobile communication terminal so that personal financial information stored in the IC card chip is maintained in a locking state; and if it is determined that the SMS message received by the mobile communication terminal is the chip blocking unlocking SMS message, driving the internal chip driver of the mobile communication terminal to permit access to the embedded or external IC card chip of the mobile communication terminal so that the personal financial information stored in the IC card chip is unlocked.

Description of drawings

Fig. 1 shows a structure of a system for locking/unlocking a mobile banking function according to an embodiment of the present invention; and

Fig. 2 is a flowchart showing a method of locking/unlocking a mobile banking function according to another embodiment of the present invention.

<Explanation of Reference numerals designating the Major Elements of the Drawings>

10: mobile communication terminal

11: IC card chip

12: chip driver

20: wireless base station

30: SMSC

40: common carrier banking server

50: financial organ host

Best Mode

Hereinafter, exemplary embodiments of the present invention will be described with reference to the accompanying drawings.

Referring to Fig. 1, a mobile communication terminal 10 includes an embedded or external IC card chip 11 in which personal financial information for supporting a banking function is stored. When the mobile communication terminal 10 receives a chip blocking SMS message for maintaining the personal financial information stored in the IC card chip 11 in a locking state, the mobile communication terminal 10 restricts access to the IC card chip 11 by driving an internal chip driver 12. When the mobile communication terminal 10 receives a chip blocking unlocking SMS message for unlocking the locking state of the personal financial information, the mobile communication terminal 10 permits access to the IC card chip 11 by driving the chip driver 12.

The chip driver 12 embedded in the mobile communication terminal 10 restricts or permits access to the IC card chip 11 of the mobile communication terminal 10 when the mobile communication terminal 10 receives a chip blocking SMS message or a chip blocking unlocking SMS message and requests chip blocking or chip blocking unlocking.

A common carrier banking server 40 communicates with the mobile communication terminal 10 via a wireless base station 20 and a short message service center (SMSC) 30 and transmits a chip blocking SMS message or a chip blocking unlocking SMS message to the mobile communication terminal 10 when receiving a chip blocking or chip blocking

unlocking request from a financial organ issuing the IC card chip.

A financial organ host 50 transmits a chip blocking request to the common carrier banking server 40 when a theft and loss report is filed by a user of the mobile communication terminal 10. When the financial organ host 50 receives a request for the reuse of the mobile communication terminal 10 for which a theft and loss report has been filed from the user, the financial organ host 50 transmits a chip blocking unlocking request to the common carrier banking server 40.

The system for locking/unlocking a mobile banking function having the above structure according to the present invention is operated using a method of locking/unlocking a mobile banking function shown in Fig. 2.

Referring to Fig. 2, when a mobile communication terminal 10 including an IC card chip 11, such as an embedded or external smart card chip or a traffic card chip storing personal financial information for supporting a banking function is stolen or lost, a user files a theft or loss report to a corresponding common carrier or a corresponding financial organ.

In addition, when the user has found the corresponding mobile communication terminal 10 after filing a theft and loss report of own mobile communication terminal 10, the user requests the reuse of the mobile communication terminal 10 for which a theft and loss report has been filed to the common carrier or the financial organ.

In particular, when the user has filed a theft and loss report not to the financial organ but to the corresponding common carrier and requests for the reuse of the mobile communication terminal 10 for which the theft and loss report has been filed, the common carrier banking server 40 receives the theft and loss report or the request for the reuse of the mobile communication terminal 10 and then transmits the contents of receipt to the

financial organ host 50.

When the financial organ host 50 receives the theft and loss report from the user or the common carrier banking server 40 or the request for the reuse of the mobile communication terminal 10 for which the theft and loss report has been filed, in step S10, the financial organ host 50 requests chip blocking or chip blocking unlocking of the common carrier banking server 40.

In this case, in step S20, the common carrier banking server 40 transmits a chip blocking SMS message including a mobile communication terminal number, a serial number of an IC card chip of a corresponding mobile communication terminal 10, and a chip blocking command to the corresponding mobile communication terminal 10 via a PSDN 30 and a wireless base station 20 or transmits a chip blocking unlocking SMS message including the mobile communication terminal number, the serial number of the IC card chip of the corresponding mobile communication terminal 10, and the chip blocking unlocking command to the corresponding mobile communication terminal 10 to the corresponding mobile communication terminal 10.

Accordingly, in step S30, the mobile communication terminal 10 determines whether or not the SMS message received from the common carrier banking server 40 is the chip blocking SMS message or the chip blocking unlocking SMS message.

If it is determined that the SMS message received by the mobile communication terminal 10 is the chip blocking SMS message, the mobile communication terminal 10 requests chip blocking of the internal chip driver 12. As a result, in step S40, the chip driver 12 drives to restrict access to the embedded or external IC card chip 11 of the mobile communication terminal 10 so that personal financial information stored in the IC card chip 11 is maintained in a locking state.

On the other hand, if it is determined that the SMS message received by the mobile communication terminal 10 is the chip blocking unlocking SMS message, the mobile communication terminal 10 requests chip blocking unlocking of the internal chip driver 12. As a result, in step S50, the chip driver 12 drives to permit access to the embedded or external IC card chip 11 of the mobile communication terminal 10 so that the personal financial information stored in the IC card chip 11 is unlocked.

As above, in the system for locking/unlocking a mobile banking function according to the present invention, the common carrier banking server 40 performs remote control on the mobile communication terminal 10 by a user's request or the request of the financial organ host 50 such that access to the IC card chip 11 of the mobile communication terminal 10 is restricted or permitted.

Industrial Applicability

As described above, in the system for locking/unlocking a mobile banking function according to the present invention, personal financial information stored in an IC card chip of a mobile communication terminal for storing personal financial information for supporting a banking function is maintained in a locking state using a short message service (SMS) message to disable access to the IC card chip or is unlocked to enable access to the IC card chip, such that when the mobile communication terminal is lost or stolen, an attempt for an illegal banking function using the IC card chip of the mobile communication terminal is completely prevented.

In addition, in the method of locking/unlocking a mobile banking function according to the present invention, a mobile communication terminal user does not need to visit a financial organ personally and needs to simply file a report to a corresponding

financial organ or common carrier such that the use of an IC card chip of the mobile communication terminal is stopped or the IC card chip is reused.

While the present invention has been particularly shown and described with reference to exemplary embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the spirit and scope of the invention as defined by the following claims.

CLAIMS

WHAT IS CLAIMED IS:

1. A system for locking/unlocking a mobile banking function, the system comprising:

a mobile communication terminal (10), which includes an embedded or external IC card chip(11) in which personal financial information for supporting a banking function is stored, when the mobile communication terminal (10) receives a chip blocking SMS message for maintaining the personal financial information stored in the IC card chip (11) in a locking state, the mobile communication terminal (10) restricting access to the IC card chip (11) by driving an internal chip driver (12), and when the mobile communication terminal (10) receives a chip blocking unlocking SMS message for unlocking the locking state of the personal financial information, the mobile communication terminal (10) permitting access to the IC card chip (11) by driving the chip driver (12);

a common carrier banking server (40), which communicates with the mobile communication terminal (10) via a wireless base station (20) and a short message service center (SMSC) (30) and transmits a chip blocking SMS message or a chip blocking unlocking SMS message to the mobile communication terminal (10) when receiving a chip blocking or chip blocking unlocking request from a financial organ issuing the IC card chip; and

a financial organ host (50), which transmits a chip blocking request to the common carrier banking server (40) when receiving a theft and loss report from a user of the mobile communication terminal (10), and which transmits a chip blocking unlocking request to the common carrier banking server (40) when receiving a request for the reuse of the mobile

communication terminal (10) for which a theft and loss report has been filed from the user.

2. The system according to Claim 1, wherein the chip driver (12) embedded in the mobile communication terminal (10) restricts or permits access to the IC card chip (11) of the mobile communication terminal (10) when the mobile communication terminal (10) requests chip blocking or chip blocking unlocking after receiving a chip blocking SMS message or a chip blocking unlocking SMS message.

3. The system according to Claim 1, wherein the common carrier banking server (40) transmits the contents of receipt to the financial organ host (50) when receiving a theft and loss report of the mobile communication terminal (10) from a user of the mobile communication terminal (10) or receiving a request for the reuse of the mobile communication terminal (10) for which the theft and loss report has been filed from the user.

4. The system according to Claim 1, wherein the financial organ host (50) transmits a chip blocking request to the common carrier banking server (40) when receiving the theft and loss report of the user of the mobile communication terminal (10) from the common carrier banking server (40) and transmits a chip blocking unlocking request to the common carrier banking server (40) when receiving a request of the reuse of the mobile communication terminal (10) for which the theft and loss report has been filed from the common carrier banking server (40).

5. A method of locking/unlocking a mobile banking function, the method comprising:

(S10) when receiving a theft and loss report of a mobile communication terminal (10) from a user of the mobile communication terminal (10) or receiving a request for the reuse of the mobile communication terminal (10) for which the theft and loss report has been filed from the user, requesting chip blocking or chip blocking unlocking of a common carrier banking server (40);

(S20) transmitting a chip blocking short message service (SMS) message or a chip blocking unlocking SMS message to the corresponding mobile communication terminal (10) via a wireless base station (20) and a PSDN (30);

(S30) determining whether or not the SMS message received from the common carrier banking server (40) is the chip blocking SMS message or the chip blocking unlocking SMS message;

(S40) if it is determined that the SMS message received by the mobile communication terminal (10) is the chip blocking SMS message, driving an internal chip driver (12) of the mobile communication terminal (10) to restrict access to an embedded or external IC card chip (11) of the mobile communication terminal (10) so that personal financial information stored in the IC card chip (11) is maintained in a locking state; and

(S50) if it is determined that the SMS message received by the mobile communication terminal (10) is the chip blocking unlocking SMS message, driving the internal chip driver (12) of the mobile communication terminal (10) to permit access to the embedded or external IC card chip (11) of the mobile communication terminal (10) so that the personal financial information stored in the IC card chip (11) is unlocked.

Fig. 1

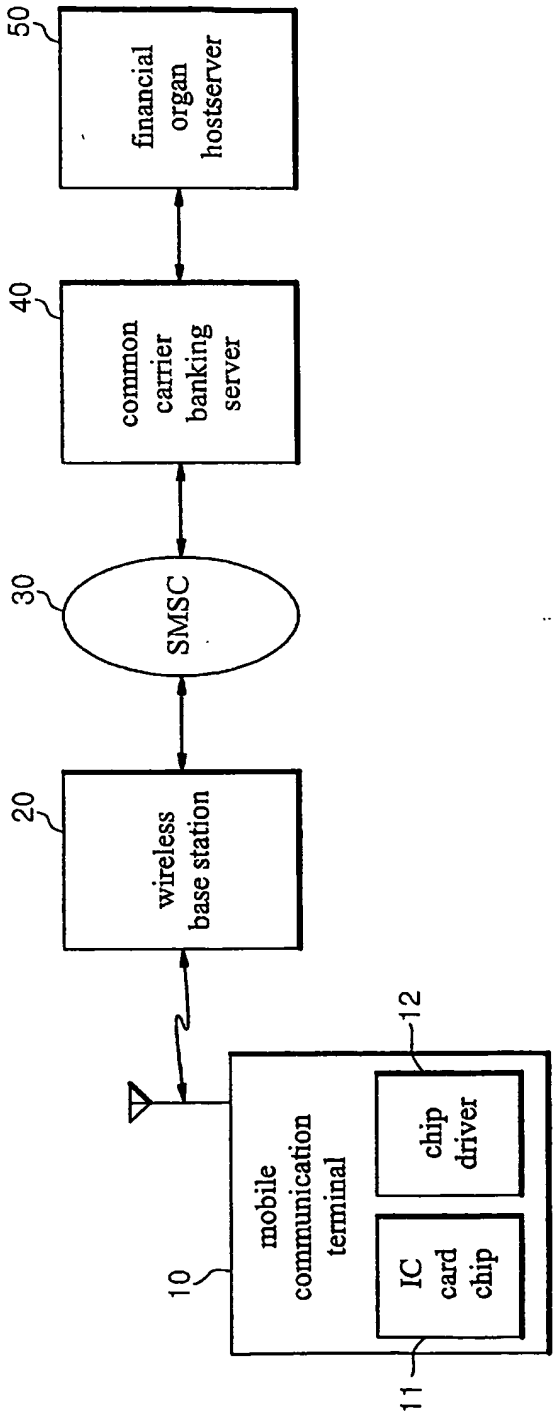
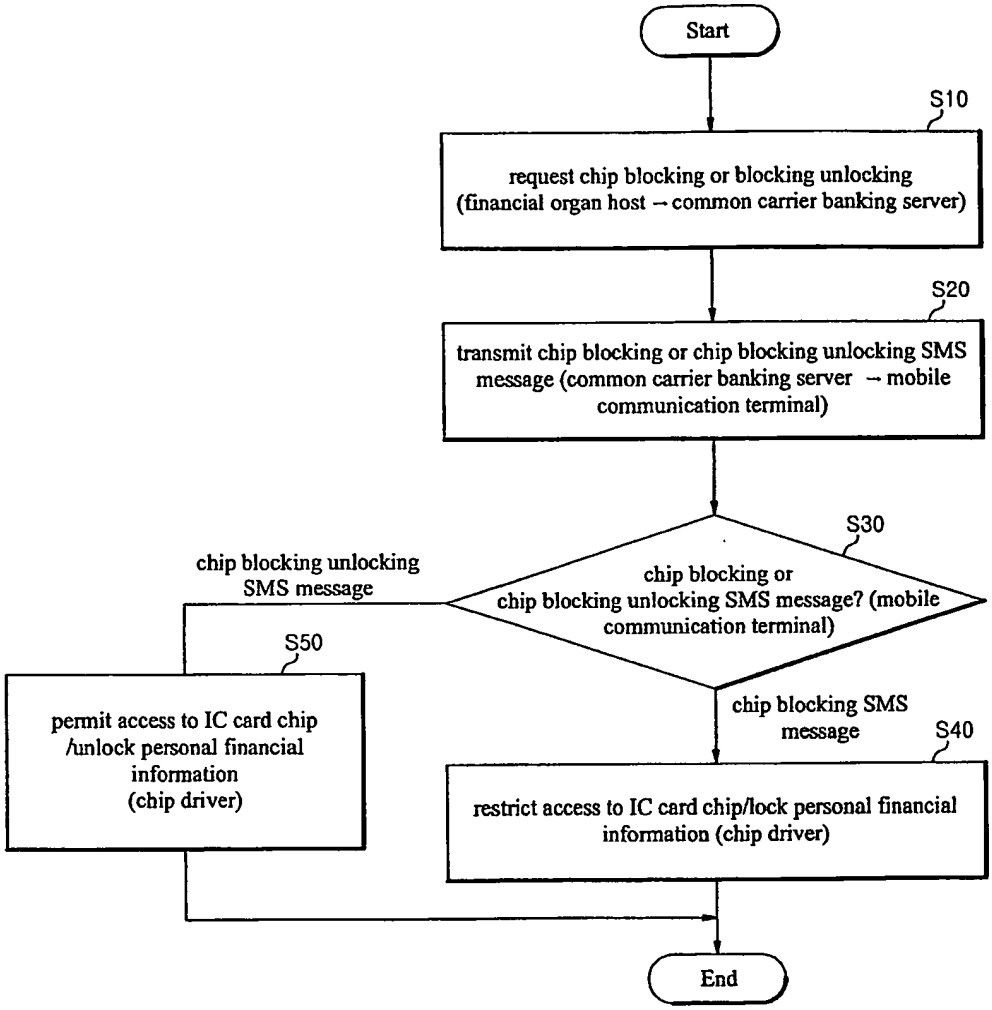

50
financial organ hostserver
40
common carrier banking server
30
SMSC
20
wireless base station
12
chip driver
IC card chip
mobile communication terminal
10
11

Fig. 2


Start
S10
request chip blocking or blocking unlocking (financial organ host → common carrier banking server)
S20
transmit chip blocking or chip blocking unlocking SMS message (common carrier banking server → mobile communication terminal)
S30
chip blocking or chip blocking unlocking SMS message? (mobile communication terminal)
chip blocking unlocking SMS message
S50
permit access to IC card chip /unlock personal financial information (chip driver)
chip blocking SMS message
S40
restrict access to IC card chip/lock personal financial information (chip driver)
End

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2004/001497

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04Q 7/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7 G06F, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 14-334210 A (SONY) Nov 22 2002 the whole document	1 - 5
A	JP 14-366858 A (SUMITOMOMITSUI) Dec 20 2002 the whole document	1 - 5

[ ] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 SEPTEMBER 2004 (15.09.2004)	**17 SEPTEMBER 2004 (17.09.2004)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea	PARK, YONG MIN
Facsimile No. 82-42-472-7140	Telephone No. 82-42-481-8120

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR2004/001497

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 14-334210 A	Nov 22 2002	None	
JP 14-366858 A	Dec 20 2002	None	